UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/815,222 | 03/31/2004 | Andrew Ginter | VRS-00101 | 7200 |

7590 10/04/2006

Muirhead and Saturnelli. LLC
200 Friberg Parkway
Suite 1001
Westborough, MA 01581

| EXAMINER | |
|---|---|
| VU, VIET DUY | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2154 | |

DATE MAILED: 10/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/815,222 | GINTER ET AL. | |
| | Examiner | Art Unit | |
| | Viet Vu | 2154 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *18 August 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *121-166 and 175-188* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *121-166,175-179,181-183 and 185-188* is/are rejected.

7)☒ Claim(s) *180 and 184* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**Art Rejections:**

1. The text of 35 USC 103(a) not cited here can be found in the previous office action.

2. Claims 121-127, 129-133, 141-148, 150-154, 162-166, 175-179, 181-183 and 185-188 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kronenberg et al, U.S. pat. Appl. Pub. No. 2004/0030778, in view of Varga et al, U.S. pat. No. 6,181,981.

Per claims 121-124, Kronenberg discloses a method and system for monitoring an industrial network comprising:

**a)** providing a plurality of agents for executing at a first computer system (120) in an industrial network (see page 3, par. 46),

**b)** reporting first data about the first computer system by a first agent executing on the first computer system in the industrial network to a controlling site (NOS), the first computer system performing at least one of: monitoring or controlling a physical process of said industrial network such as file monitoring, log file, login, etc., (see page 2, par. 37-39).

Kronenberg also teaches using other alternate communication links e.g., out-of-band communication links, in case to the

network communication failure for sending a report/alert to the controlling site (see page 2, par. 40).

Kronenberg does not explicitly teach sending data over a one-way communication link. The use of one-way communication for sending data to a remote controlling site is well known in the art as disclosed by Varga (see Varga in col 6, lines 45-50).

It would have been obvious to one of ordinary skill in the art to utilize one-way communication in Kronenberg for sending report/alert to the controlling site in case of network communication failure because it would have provided an economical backup communication link for sending report to the data collection/monitoring center (see Varga in col 6, lines 45-50).

Kronenberg does not explicitly teach reporting information about software used in connection with a particular physical process. It is however noted that many applications at the monitored sites are software-based applications, e.g., authentication, firewalls, network traffic monitoring, etc., (see page 2, par. 37).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to realize such software information reporting in Kronenberg because it would have

enabled identifying the problems associated with the (software-based) applications (see page 2, par. 39 and page 5, par. 73).

Per claims 125-127, 177 and 181, Kronenberg teaches that the software agents include a master agent (RMS server) and other software agents for performing a set of monitoring tasks (see page 2, par. 38).

Per claims 129-131, Kronenberg teaches using a state transition or event-based model that monitors (open/closed) status of a connection port to detect a drop of connection or a new connection (see page 8, par. 109). It would have been obvious to one skilled in the art to utilize such monitored information for a performance analysis application, e.g., number of reported open/closed ports that appear abnormal (see page 4, par. 52).

Per claims 132-133, Kronenberg teaches using logic or set of rules to detect and generate an alert/report regarding a potential problem or anomaly at the monitored site (see page 5, par. 73).

Per claim 141, Kronenberg teaches processing and sending periodical report (see page 6, par. 78). Kronenberg does not explicitly teach applying particular rule for sending the report such as a predetermined data size or a fixed report schedule.

It would have been obvious to one skilled in the art at the time the invention was made to apply any arbitrary rule to the report data including size of the report and time for sending the report because such rules would have enabled processing the report more easily.

Per claims 178 and 182, it is noted that it is well known in the art that connection is initiated at the application layer

Per claims 179 and 183, it is also noted that it is well known in the art that data packets are processed at the network layer.

Per claims 185-186 and 187-188, Kronenberg teaches using RMS to process the data reported by other software agent and transmitting notifications to the remote controlling site (see page 2, par. 39).

Claims 142-148, 150-154, 162-166 and 175-176 are similar in scope as that of claims 121-127, 129-133 and 141.

3. Claims 128, 134-140, 149 and 155-161 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kronenberg and Varga, and further in view of Schlossberg et al, U.S. pat. Appl. Pub. No. 2002/00660034.

Kronenberg does not explicitly teach handling specific attacking attempts monitored at the security device, e.g.,

firewall. Schlossberg teaches a network security system for detecting and handling network attacks. Particularly, Schlossberg discloses:

**a)** detecting suspicious activity in the network (see Schlossberg in page 5, par. 53-54),

**b)** performing data matching to determine events of interest and assessing a level of threat (see Schlossberg in page 7, par. 63),

**c)** creating a message for reporting to the management unit,

**d)** encrypting the message before sending the message (see Schlossberg in page 8, par. 74),

**e)** decrypting the received message (see Schlossberg in page 7, par. 60 and fig. 7).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Kronenberg with Schlossberg's teaching because it would have enabled sufficient handling of network attacks in Kronenberg.

Per claims 135-136 and 156-157, Schlossberg teaches blocking access or shutting down the device, e.g., firewall, in response to an identified attack (see Schlossberg in page 8, par. 76). It is noted that such changes in operation would reflect on the device configuration.

It would have been further obvious to one of ordinary skill in the art at the time the invention was made to recognize that log data would include any such changes in operation of the device.

**Allowable Subject Matter:**

4. Claims 180 and 184 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

**Response to Amendment:**

5. Applicant's arguments filed on 7/17/06 with respect to claims 121-166 and 175-188 have been fully considered but they are not deemed persuasive.

Per claims 121 and 142, applicant asserts that one-way communication would have not been operable in Kronenberg because Kronenberg requires a two-way communication between the RMS server and the agents at the client site.

The examiner submits that the office action has been revised to clearly propose the use of one-way communication between the client site (first computer system) and the central monitoring server instead of between the RMS server and the

software agents. As discussed above, Kronenberg teaches using an alternate out-of-band communication link for transmitting data to the remote controlling server in case to network failure (page 2, par. 40). Such use of one-way communication as an alternate communication in Kronenberg would have been obvious to one skilled in the art because of its lower operating cost.

Per claims 125-126, applicant alleges that Kronenberg fails to teach executing a master agent and other agents at the monitored site.

The examiner disagrees. As discussed above, the monitored site is now defined as the client site comprising RMS server, software agents and other sensors for monitoring physical processes at the client.

Per claims 132-133, applicant alleges that Kronenberg does not teach using set of rules to generating a report.

The examiner disagrees. Kronenberg teaches using logic or set of rules to detect and generate an alert/report regarding a potential problem or anomaly at the monitored site (see page 5, par. 73).

**Conclusion:**

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Viet Vu whose telephone number is 571-272-3977. The examiner can

normally be reached on Monday through Thursday from 8:00am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee, can be reached on 571-272-3964.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit 2154
9/29/06

VIET D. VU
PRIMARY EXAMINER